(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 October 2002 (24.10.2002)

PCT

(10) International Publication Number
WO 02/084602 A1

(51) International Patent Classification[7]: G07C 9/00, G07F 7/10

(21) International Application Number: PCT/EP02/04235

(22) International Filing Date: 17 April 2002 (17.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1017856 17 April 2001 (17.04.2001) NL

(71) Applicant and
(72) Inventor: VAN DER VELDEN, Hendrikus, Hermanus [NL/NL]; Chopinstraat 45, NL-8031 ZH Zwolle (NL).

(74) Agent: BARTELDS, Erik; Arnold & Siedsma, Sweelinckplein 1, NL-2517 The Hague (NL).

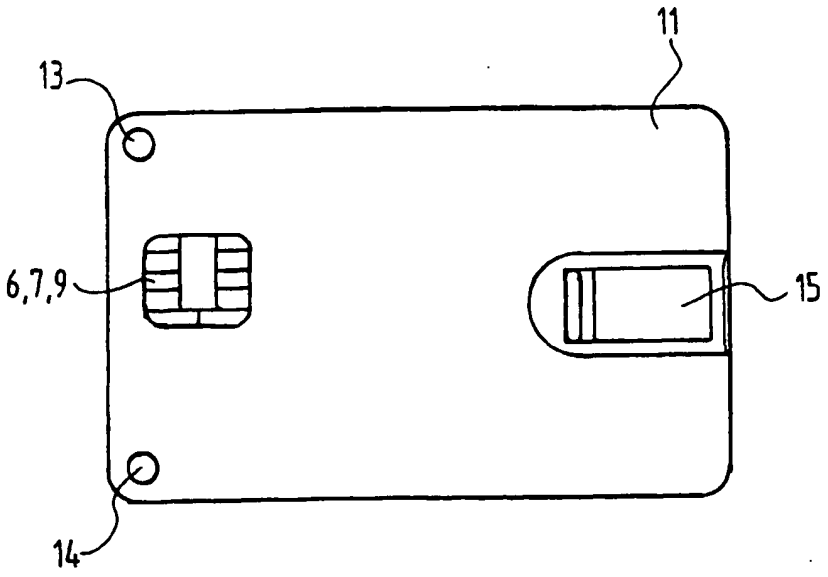
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR IDENTIFYING A PERSON BY USING BIOMETRIC CHARACTERISTICS



(57) Abstract: The invention relates to a method for identifying a person, e.g. for use in controlling access ot physical or virtual spaces. The method comprises the steps of storing data relating to the identity of the person in first memory means, storing data relating to at least one unique biometric characteristic of the person in second memory means, detecting the at least one biometric characteristic on demand, comparing the or each detected biometric characteristic with the or each stored biometric characteristic, and releasing the identity data when the or each detected biometric characteristic matches the or each stored biometric characteristic. By using biometric characteristics,like, e.g. a fingerprint, an image of an iris or a DNA-"fingerprint", which are unique to each person, the results of the identification cannot be manipulated, thereby providing excellent security. the invention also relates to a system for carrying out this method. In a preferred embodiment of the system, the memory means are arranged on a card together with the comparing means and possibly the detecting means, resulting in an extremely compact, very secure self contained personal identification system.

WO 02/084602 A1

METHOD AND SYSTEM FOR IDENTIFYING A PERSON BY USING BIOMETRIC CHARACTRISTICS

The present invention relates to a method and system for identifying persons on the basis of unique biometric characteristics, and more specifically to such method and system using cards on which the biometric characteristics are stored in electronic form in combination with scanners for detecting the biometric characteristics of a person carrying the card.

There is an increasing need for efficient methods and systems for personal identification. Personal identification systems are in widespread use, e.g. for controlling access to restricted areas, both physical and virtual, and for allowing people to perform transactions, specifically financial transactions.

A classic example of a personal identification system is the use of tags or badges provided with the name and/or a photograph of the bearer. Such systems require the use of personnel for checking the identity of the bearer, and are therefore expensive. Moreover, the involvement of personnel means that such systems are not well suited for applications where users should be able to gain access around the clock. Finally, such systems are obviously ill suited for remote access control.

Therefore, organisations increasingly rely on fully automated personal identification systems. Most automated systems are based on the use of passwords or personal identification numbers (PIN's), either chosen by a user or issued by an organisation, which must be entered before gaining access or being allowed to perform certain transactions. These passwords or PIN's are stored in a central database, which must then be contacted and queried

every time the password or PIN is used. This kind of system is generally used for controlling access to computer networks and for performing financial transactions from remote terminals. In the latter case the user carries a card provided with a magnetic strip containing information identifying the user, like, e.g. his bank account number. After presenting this card to the terminal and entering his password or PIN, the user may perform a payment at the terminal.

These known personal identification systems have the drawback that passwords or PIN's issued by an organisation are usually too complex to remember correctly under all circumstances, so that users tend to write them down. If users are allowed to choose their own password or PIN, these are usually obvious combinations of characters, like, e.g. names or birthdays, and thus fairly simple to decipher. Therefore, security is often compromised in password based personal identification systems, which leads to fraud and abuse, resulting in huge damages, especially in the case of financial systems. Moreover, such systems tend to be slow at peak times, as all passwords that are entered must be sent to the central database for processing. Finally, the use of a central database for controlling and authorizing transactions raises issues of privacy.

The invention therefore has for its object to provide an automated method and system for personal identification that are more secure than present methods and systems.

A further object of the invention is to provide a personal identification method and system which do not rely on a central database, i.e. a stand alone method and system, which are thus quicker and more efficient than prior art methods and systems.

Yet another object of the invention is the provision of a method and system in which the personal identification is based on information that cannot be manipulated.

To this end the present invention provides a method for identifying a person, comprising the steps of storing data relating to the identity of the person in first memory means, storing data relating to at least one unique biometric characteristic of the person in second memory means, detecting the at least one biometric characteristic on demand, comparing the or each detected biometric characteristic with the or each stored biometric characteristic, and releasing the identity data when the or each detected biometric characteristic matches the or each stored biometric characteristic. By using biometric characteristics, like, e.g. a fingerprint, an image of an iris or a DNA-"fingerprint", which are unique to each person, the results of the identification cannot be manipulated, thereby providing excellent security.

Preferably, the first and second memory means are portable, and the comparison is made by portable comparing means connected to the second memory means. Moreover, the detection may be performed by portable detecting means connected to the comparing means. In a preferred embodiment, the first and second memory means, the comparing means and the detecting means are arranged on a common carrier. In this way the user can carry along his personal identification kit, which may be shaped and dimensioned like a credit card.

To further enhance security, it is preferred that multiple biometric characteristics, e.g. at least one external and at least one internal biometric characteristic, are stored, detected and compared. Examples of such combinations of internal and external biometric characteristics may be a fingerprint and a pattern of

subcutaneous blood vessels, a fingerprint and a pressure exerted by the finger, or a fingerprint and a temperature of the finger. Obviously, when a different external biometric characteristic is used for identification, like e.g. the iris, different internal biometric characteristics may be used as well.

If the at least one biometric characteristic is detected in a static manner, the demands on the system in terms of scanning and processing speeds may be limited, thus allowing the use of relatively simple and low-cost components. On the other hand, the risk of manipulation after scanning may be reduced when the at least one biometric characteristic is detected in a dynamic manner, e.g. when inserting the card into a terminal.

In order to allow an accurate detection of the biometric characteristic(s), without requiring excessive capacity of the memory means and/or comparing means, it is preferred that during detection of the at least one biometric characteristic a great number of data is generated, while only part of the generated data is stored and compared. This may be achieved e.g. by detecting a pattern in the generated data, and storing and comparing only this pattern.

An efficient and easy-to-use method is obtained, when the released identity data are transmitted in a wireless manner.

In order to allow the method to be used for verifying access authority, rather than the actual identity of the user, the identity data preferably comprise an access code.

Compatibility with existing practices is guaranteed, when the steps of storing, detecting, comparing and/or releasing are performed electronically. Moreover, this allows the method to be implemented using off the shelf low-cost components.

The invention also provides a system for identifying a person. The inventive system comprises first memory means for storing data relating to the identity of the person, second memory means for storing data relating to at least one unique biometric characteristic of the person, means for detection on demand of the at least one biometric characteristic, means connected to the second memory means and the detection means for comparing the or each detected biometric characteristic with the or each stored biometric characteristic, and means connected to the comparing means for releasing the identity data from the first memory means when the comparing means indicate that the or each detected biometric characteristic matches the or each stored biometric characteristic.

Preferably, the system includes means for displaying the released identity data, which may include an image of the user. In this way the card on which the various data are stored may be used as an identity card, like, e.g. a passport, which may be checked by security personnel.

In case the identity data comprise an access code the system is preferably arranged for allowing access to certain areas and/or granting permission for performing certain acts in response to the released access code.

An efficient system architecture is obtained when the first and second memory means are integrated.

Preferably, the detecting means comprise an array of electronic detecting elements, allowing an electronic "image" of the biometric characteristic(s) to be made. Each detecting element may supply an electrical signal, while the memory means and comparing means are preferably arranged for storing and comparing only part of the supplied electrical signals, whereby a comparatively high processing speed may be maintained using relatively simple components.

In order to allow for efficient processing of the supplied signals using digital electronics, the system may include means arranged between the electronic detecting elements and the memory means for digitizing the supplied electrical signals.

Finally, the invention provides a carrier, specifically a card, for use in a system as defined above.

The above and other objects, features and advantages of the present invention will be better understood upon reading the following detailed description of preferred embodiments thereof, in conjunction with the annexed drawings, in which:

Fig. 1 is a schematic perspective view of computer network including a plurality of remote terminals connected to a central host computer, with which the personal identification system of the present invention can be used,

Fig. 2 is a schematic block diagram of various essential components of the system of the present invention,

Fig. 3 is a flow sheet showing the various steps of the method of the invention,

Fig. 4 is a schematic block diagram of a biometric scanner for use in the system of the invention,

Fig. 5 represents a pattern that is derived from data generated by the biometric scanner,

Figs. 6 and 7 are pictorial views of alternative embodiments of cards for use in the system of the invention, including scanners for static and dynamic detection, respectively,

Fig. 8 is a schematic perspective view showing a fingerprint being dynamically detected during insertion of the card of fig. 7 into a slot, and

Fig. 9 is a schematic representation of a wireless embodiment of the personal identification system.

Fig. 1 shows a computer network 1 including one or more central host computers 2 and a plurality of terminals 3, from where the computer network 1 and the central host computers 2 may be accessed through modems 4. The network 1 may for instance be used by clients of a bank or credit card company for performing electronic financial transactions, e.g. making payments from an account held at the bank, retrieving cash from an ATM, etc. Access to the network 1 is controlled by a personal identification system 5, which verifies the identity of users and their authority to perform certain transactions.

The personal identification system 5 of the present invention is based on matching one or more biometric characteristics of a user presenting himself at a terminal 3 to biometric characteristics stored in a memory and associated with data relating to the identity of the "owner" of these biometric characteristics. The biometric characteristic may be a fingerprint, the shape and colour of the iris of an eye, a DNA-"fingerprint", etc. Because such biometric characteristics are unique to each and every person, they allow a one hundred percent reliable identification to be performed.

Fig. 2 shows the essential elements of the personal identification system 5 of the invention. The system 5 includes first memory means 6 for storing data relating to the identity of the user and second memory means 7 for storing data relating to at least one unique biometric characteristic of the user. The system 5 also includes means 8 for detecting the biometric characteristic(s) and comparing means 9 connected to the second memory means 7 and the detecting means 8. These comparing means 9 are arranged for comparing the detected biometric characteristic(s) with the stored biometric characteristic(s) and for providing a

release signal when the detected biometric characteristic(s) match(es) the stored biometric characteristic(s). Finally, the system 5 is provided with release means 10 connected to the comparing means 9 and acting on the first memory means 6 for releasing the identity data from the first memory means 6 when supplied with the release signal from the comparing means 9.

In order to render the system 5 independent from the network 1 and central host computer(s) 2, the comparison between the stored and detected biometric characteristic(s) may take place at the remote terminals 3. Preferably, however, this comparison is performed on a carrier 11, which may be shaped and dimensioned like a credit card, and which the user may carry with him. To this end, the first 6 and second 8 memories, containing the identity data and biometric data, respectively, and the comparing means 9 are all arranged on the card-shaped carrier 11. These components may all form part of a single integrated circuit realized in CMOS technology for reduced power consumption.

Also, the detection of the user's biometric characteristic(s) may be performed by a scanner 12 connected to or forming part of the terminal 3. In a preferred embodiment of the invention, however, such scanning is also done on the card-shaped carrier 11 itself, so that this carrier 11 constitutes a self contained personal identification system 5. This preferred embodiment requires the detecting means 8 to be thin, compact and light-weight, and to have a low power consumption. An example of a fingerprint scanner meeting these requirements will be described below with reference to fig. 4.

When a user is first registered in the personal identification system, his relevant biometric characteristic(s) is/are determined once, e.g. by scanning.

This may be performed either by the detecting means 8, or by a separate scanner. The results of this determination are stored in the second memory 7. At the same time, data relating to the identity of the user are registered and stored in the first memory 6. Depending on the use of the system 5, the identity data may include personal data of the user, like his name, date of birth, marital status, etc.; related data, like the user's home address, place of work, etc.; financial data relating to bank accounts, credit card numbers, insurance policies, etc., or even medical files. The identity data may also include one or more images of the user, so that the card may be used as an ID-card that can be checked by security personnel. However, it is also conceivable that the identity data comprise only an access code, possibly determining a level of authority, without any actual data personally identifying the user. In this way the system may be used as an access control system only.

After the registration is completed, every time the user wishes to gain access to the computer network or wishes to perform certain transactions at the terminal, the relevant biometric characteristic(s) is/are detected again by the detecting means 8 (step 1 in fig. 3). Then the stored biometric characteristic(s) is/are read from the second memory 7 (step 2). Subsequently, the detected biometric characteristic(s) is/are compared with the characteristic(s) read from the second memory 7 (step 3). When this comparison results in a match, the identity data that are stored in the first memory 6 are released (step 4a). If, on the other hand, no match is found, an error signal is generated, and the identity data are not released (step 4b). This error signal may be used to display an error message, or to illuminate a red LED 13 on the card 11, as in the preferred embodiment illustrated in figs. 6 and 7. In this embodiment, a

successful match results in a green LED 14 being illuminated (step 4c).

In order to minimize the demands on the comparing means 9, which may be constituted by a CPU forming part of a single IC with the memories 6, 7, the data generated during the detecting step may be compressed or reduced before being sent to the comparing means 9. To this end a conventional data compression algorithm may be used, which may be implemented in a data compression circuit arranged between the detecting means 8 and the comparing means 9. However, in a preferred embodiment of the invention, the amount of data is reduced by detecting a pattern in the data, and initially storing only this pattern or "template" for comparison with a pattern detected from the data of a subsequent scan. The pattern may be defined by a relatively small number of easily recognizable points and their mutual relationship, expressed in terms of distance and direction.

Turning now to fig. 4, in the preferred embodiment the detecting means 8 comprise an array 15 of electronic detecting elements or sensors. The sensor array 15 may for instance include 300 rows 17 and 256 columns 18 of metal electrodes, each of which may act as one plate of a capacitor. The sensor array 15 may be contacted by a finger of the user, which then acts as second plate of each capacitor. The sensor array 15 is covered by a passivation layer forming the dielectric between these two capacitor plates. Ridges and valleys on the finger, which define the fingerprint, lead to varying capacitor values across the array, and thus to variations in discharge voltage which may be read to form an image of the fingerprint.

Associated with each column 18 of the sensor array 15 are two sample-and-hold circuits 16a, 16b. In case of static detection of the biometric characteristic(s) the fingerprint

image is captured one row 17 at a time. This row capture occurs in two phases. In a first phase the sensor plates of the selected row 17 are pre-charged to a certain voltage, and these pre-charged plate voltages are stored in the first set of sample-and-hold circuits 16a. In the second phase, the row 17 is discharged with a current source, with the rate of discharge of each cell being proportional to the discharge current. After a set period of time the second set of sample-and-hold circuits 16b store the final plate voltages. The difference between the voltages stored in the two circuits 16a, 16b is a measure of the capacitance of each cell in the array 15, and therefore of the presence of a ridge or valley of the fingerprint. After a row 17 is captured, the stored values may be digitized by an A/D converter 19 for further processing by a processor 20, while the next row 17 may be captured. The processor 20 is programmed for analysing and optimizing the captured image by controlling a variety of parameters. During this analysis, the processor will disregard apparent anomalies which may be due to unusual skin conditions, like scratches, or simply to dirt. The processor 20 is further programmed to recognize and compensate for misalignment of the finger on the sensor 15. Variations of up to approximately 10° to eighter side may be accommodated in this manner.

Storing and comparing the approximately 75,000 pixels generated by the fingerprint sensor 15 would require a huge processing capacity, which is incompatible with the requirement that the entire system should be able to be implemented on a card. In order to reduce the number of data, the invention proposes to identify a limited number of easily recognizable points 24 (fig. 5) when the fingerprint is first scanned, and to store only these points 24 and their mutual relationships. These mutual relationships are expressed in

terms of distances and directions, either in orthogonal (x, y) or in polar (r, α) coordinates. By identifying e.g. as little as nine points 24a-i, and storing these points together with eight vectors 25a-h leading from one point 24 to the next as a so-called "template" 26, the fingerprint image defined by the 75,000 pixels may be stored and processed in a very efficient manner, without a significant loss of information.

Although the sensor 15 described above is suitable for detecting a two-dimensional image of a fingerprint, i.e. an external biometric characteristic, it may be desirable for additional security to also detect an internal biometric characteristic, which is even more difficult to manipulate. For instance, when reading the image of the fingerprint, an image of blood vessels running below the skin of the finger could be detected at the same time, thus leading to a "three dimensional" image being detected.

The image of the blood vessels could be formed by detecting the temperature of the fingertip at various locations. The temperature *per se* is an indication if a live finger is placed on the sensor 15, as the temperature of human beings normally ranges from about 35 to 40°C (approx. 95 to 105°F). By measuring the temperature at different locations an indication of the course of the blood vessels may be obtained, as the temperature in the blood stream will differ from that of finger tissue. The temperature and its distribution can be measured by a plurality of thermal sensors 23, e.g. spaced along the edges of the fingerprint sensor 15. In a simpler embodiment, only a single thermal sensor is used to detect if the finger belongs to a living human being.

Instead of the temperature, the pressure exerted by the finger and its distribution over the surface area of the

sensor could be detected as internal biometric characteristic. Like the temperature, this pressure is an indication of a live finger as well, as it is determined to a large extent by blood pressure in the vessels. When circulation stops, this pressure will fall and the fingerprint will be slightly altered. For detecting the pressure distribution, a plurality of pressure sensors (not shown) could be arranged under the fingerprint sensor 15.

In the above embodiment a static detection of a fingerprint was performed. However, this static detection takes some time, in the order of 2 to 4 seconds with the sensor envisaged at present. In order to accelerate the detection, an alternative embodiment of the personal identification system of the invention is provided with a so-called "swipe" sensor 21. This swipe sensor 21 detects only a relatively thin slice of a fingerprint when the finger F is swiped across its surface. As the swipe sensor 21 is smaller and has less detecting elements than the static sensor array 15, it requires less computing power for comparing the results of the detection with the biometric data stored in the memory. Moreover, the swipe sensor 21 allows the fingerprint detection to be performed while the card 11' carrying the sensor 21 is being inserted into a reader, e.g. an ATM (fig. 8). This avoids any possibility of manipulating the card 11' after the fingerprint has been detected, thus leading to even better security.

Detection of a strip of a fingerprint in the swipe sensor 21 is performed substantially in the same way as in the stationary fingerprint sensor 15. However, since the fingerprint is moved across the sensor, the number of rows of detecting elements that is required for forming an image thereof is substantially smaller. In theory, a single row of detecting elements could be sufficient, but in practice a

plurality of rows is used nevertheless, in order to provide redundancy and an enhanced fingerprint image.

In the embodiment of figs. 6 and 7, the IC containing the memories 6, 7, the comparing means 9 and the release means 10 includes contacts that are accessible at the surface of the card 11, so that the released identity data may be read when the card 11 is inserted into a reader. These contacts may also be used to supply power to the IC when the card 11 is being read. Alternatively, the card 11 may be provided with its own power supply, e.g. a small battery. This battery may be charged by means of a solar collector (not shown). The solar collector might also be the sole power source.

In an alternative embodiment, the identity data may be read without physical contact between the card 11" and the reader being required (fig. 9). The reader is an RF reader 22 in which the so-called MIFARE interface technology is implemented. This interface technology is also implemented in the release means 10 of the card 11", which in this embodiment also includes an antenna. When the card 11" is brought in the proximity of the RF reader 22, the detecting means 8, comparing means 9 and release means 10 are automatically activated, and if the scanned biometric characteristic matches the stored characteristic, the identity data released from the memory 6 are automatically sent to the RF reader 22. At the same time, the power supply on the card 11" is charged.

Although the method and system of the invention have been illustrated by means of preferred embodiments thereof, the skilled person will appreciate that many modifications and variations are possible within the scope of the invention. For instance, the biometric characteristics of several users, e.g. members of a family, could be stored in

the memory, thus allowing all these users access to a system. Different levels of authority could then be associated with the biometric data of the various users. The system could also be used to display the released identity data, so that the card could function as a passport or drivers licence, allowing officials to check the identity of the user. The identity data stored in the memory could also include the user's preferences in certain areas, allowing the card to be used as personal filter card in a system as defined in applicant's earlier patent NL 1008584. Although completely electronic embodiments have been described here, the sensor could also be an optical sensor, e.g. for performing an iris scan. The scope of the invention is therefore defined solely by the appended claims.

Claims

1. A method for identifying a person, comprising the steps of:

- storing data relating to the identity of the person in first memory means,
- storing data relating to at least one unique biometric characteristic of the person in second memory means,
- detecting the at least one biometric characteristic on demand,
- comparing the or each detected biometric characteristic with the or each stored biometric characteristic, and
- releasing the identity data when the or each detected biometric characteristic matches the or each stored biometric characteristic.

2. The method as defined in claim 1, **characterized in that** the first and second memory means are portable, and the comparison is made by portable comparing means connected to the second memory means.

3. The method as defined in claim 2, **characterized in that** the detection is performed by portable detecting means connected to the comparing means.

4. The method as defined in claim 3, **characterized in that** the first and second memory means, the comparing means and the detecting means are arranged on a common carrier.

5. The method as defined in any of the preceding claims, **characterized in that** multiple biometric characteristics are stored, detected and compared.

6. The method as defined in claim 5, **characterized in that** at least one external and at least one internal biometric characteristic is stored, detected and compared.

7. The method as defined in any of the preceding claims, **characterized in that** the at least one biometric characteristic is detected in a static manner.

8. The method as defined in any one of claims 1 to 6, **characterized in that** the at least one biometric characteristic is detected in a dynamic manner.

9. The method as defined in any of the preceding claims, **characterized in that** during detection of the at least one biometric characteristic a great number of data is generated, and only part of the generated data is stored and compared.

10. The method as defined in any of the preceding claims, **characterized in that** the released identity data are transmitted in a wireless manner.

11. The method as defined in any of the preceding claims, **characterized in that** the identity data comprise an access code.

12. The method as defined in any of the preceding claims, **characterized in that** the steps of storing, detecting, comparing and/or releasing are performed electronically.

13. A system for identifying a person, comprising:

- first memory means for storing data relating to the identity of the person,
- second memory means for storing data relating to at least one unique biometric characteristic of the person,
- means for detection on demand of the at least one biometric characteristic,
- means connected to the second memory means and the detection means for comparing the or each detected biometric characteristic with the or each stored biometric characteristic, and

- means connected to the comparing means for releasing the identity data from the first memory means when the comparing means indicate that the or each detected biometric characteristic matches the or each stored biometric characteristic.

14. The system as defined in claim 13, **characterized in that** at least the first and second memory means and the comparing means are portable.

15. The systems as defined in claim 14, **characterized in that** the detecting means are portable.

16. The system as defined in claim 15, **characterized in that** the first and second memory means, the comparing means and the detecting means are arranged on a common carrier.

17. The system as defined in claim 16, **characterized in that** the carrier has the shape of a card.

18. The system as defined in any of claims 13 to 17, **characterized in that** the second memory means, the detecting means and the comparing means are arranged for storing, detecting and comparing multiple biometric characteristics.

19. The system as defined in claim 18, **characterized in that** the detecting means are arranged for detecting at least one external and at least one internal biometric characteristic.

20. The system as defined in any of claims 13 to 19, **characterized in that** the detecting means are arranged for performing static detection.

21. The system as defined in any of claims 13 to 19, **characterized in that** the detecting means are arranged for performing dynamic detection.

22. The system as defined in any of claims 13 to 21, **characterized** by means for wireless transmission of the released identity data.

23. The system as defined in any of claims 13 to 22, **characterized** by means for displaying the released identity data.

24. The system as defined in any of claims 13 to 23, **characterized in that** the identity data comprise an access code and in that the system is arranged for allowing access to certain areas and/or granting permission for performing certain acts in response to the released access code.

25. The system as defined in any of claims 13 to 24, **characterized in that** the first and second memory means, the detection means, the comparing means and/or the releasing means comprise electronic circuitry.

26. The system as defined in claim 25, **characterized in that** the first and second memory means are integrated.

27. The system as defined in claims 25 or 26, **characterized in that** the detecting means comprise an array of electronic detecting elements.

28. The system as defined in claim 27, **characterized in that** each detecting element supplies an electrical signal, and in that the memory means and comparing means are arranged for storing and comparing only part of the supplied electrical signals.

29. The system as defined in claim 27 or 28, **characterized** by means arranged between the electronic detecting elements and the memory means for digitizing the supplied electrical signals.

30. A carrier, specifically a card, for use in a system as defined in any of claims 16 to 29.

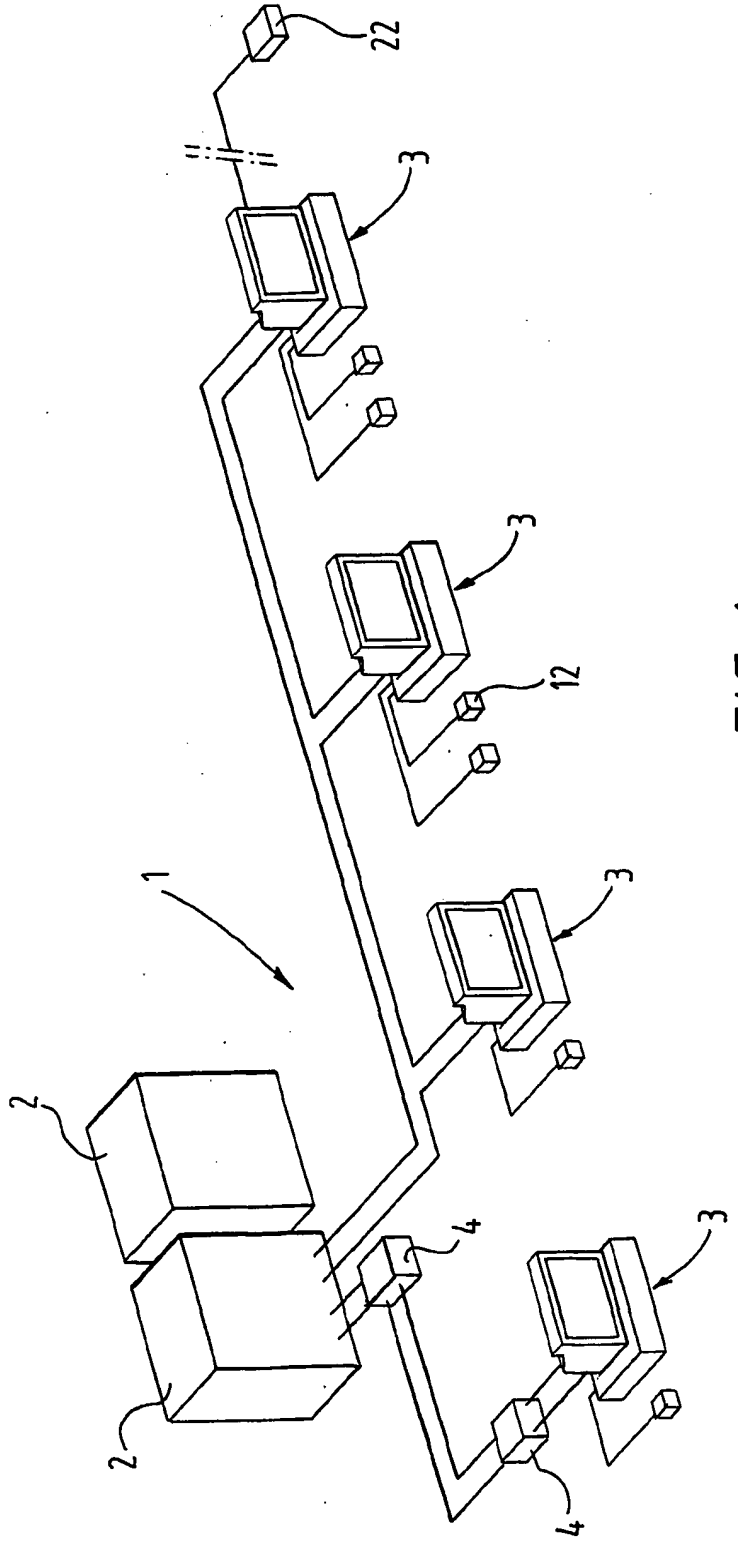


FIG. 1

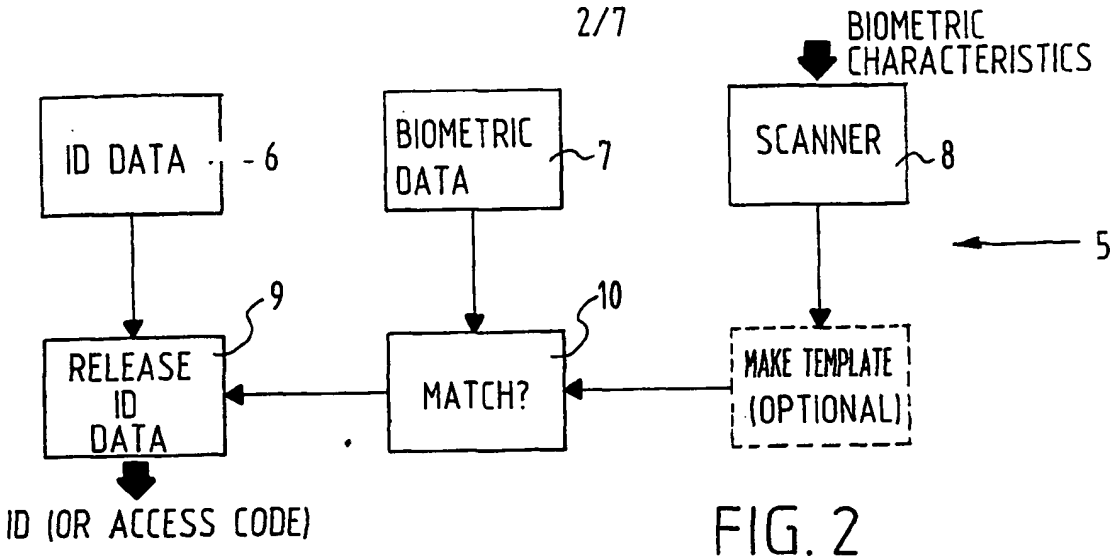

BIOMETRIC CHARACTERISTICS
ID DATA
6
BIOMETRIC DATA
7
SCANNER
8
5
9
10
RELEASE ID DATA
MATCH?
MAKE TEMPLATE (OPTIONAL)
ID (OR ACCESS CODE)

FIG. 2

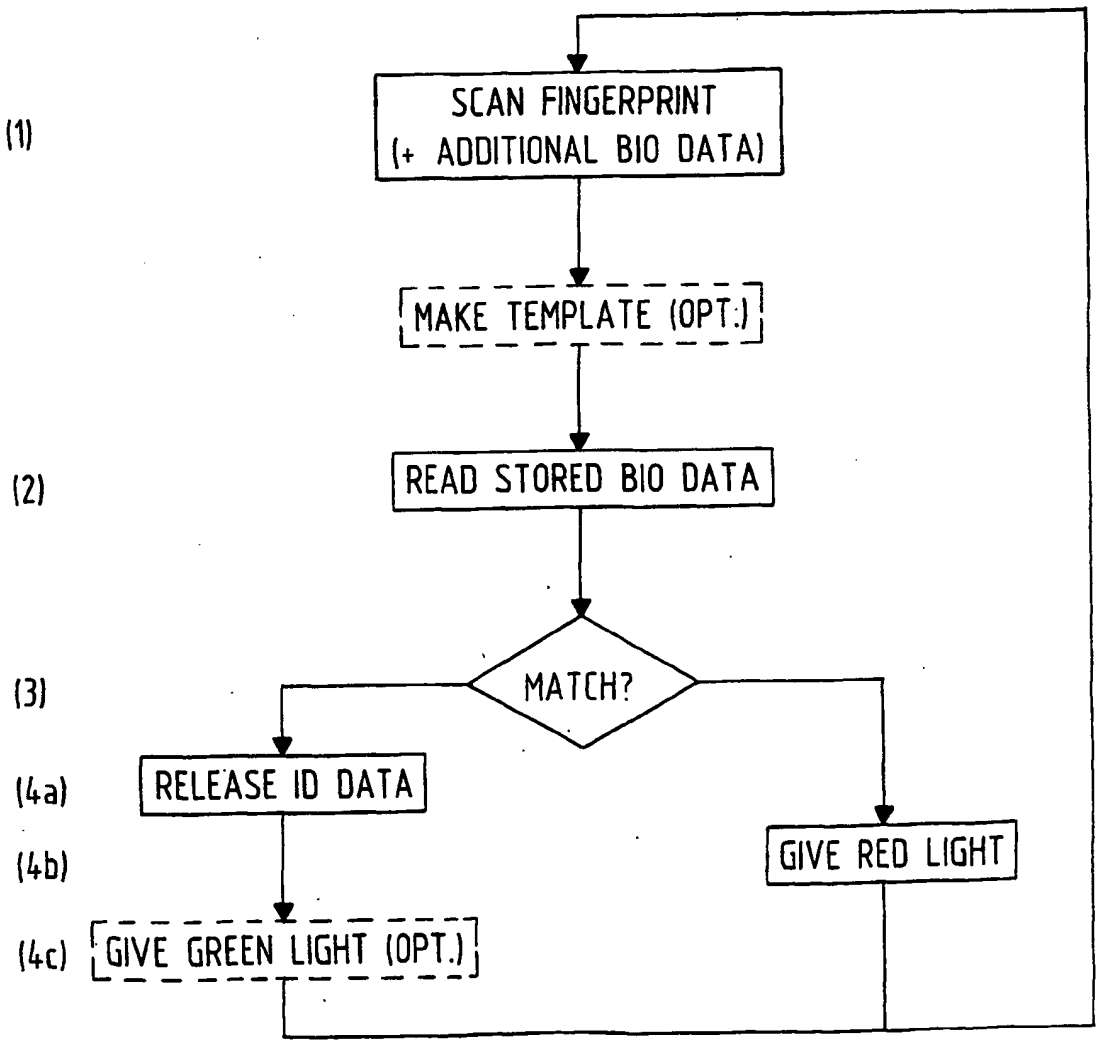

(1)
SCAN FINGERPRINT (+ ADDITIONAL BIO DATA)
MAKE TEMPLATE (OPT.)
(2)
READ STORED BIO DATA
(3)
MATCH?
(4a)
RELEASE ID DATA
(4b)
GIVE RED LIGHT
(4c)
GIVE GREEN LIGHT (OPT.)

FIG. 3

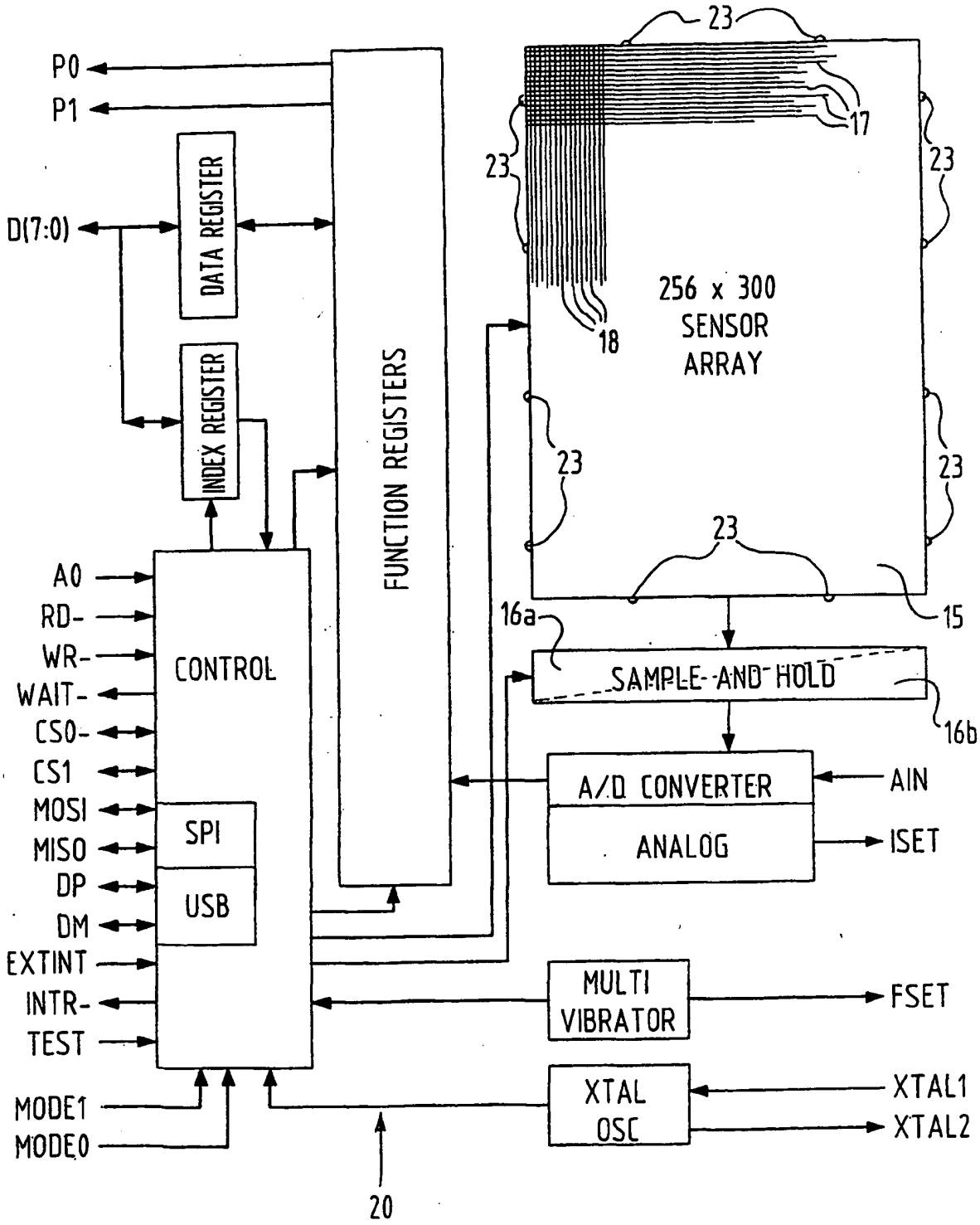

P0
P1
D(7:0)
DATA REGISTER
INDEX REGISTER
FUNCTION REGISTERS
A0
RD-
WR-
WAIT-
CS0-
CS1
MOSI
MISO
DP
DM
EXTINT
INTR-
TEST
CONTROL
SPI
USB
MODE1
MODE0
20
23
17
18
256 x 300
SENSOR
ARRAY
15
16a
16b
SAMPLE-AND-HOLD
A/D CONVERTER
AIN
ANALOG
ISET
MULTI
VIBRATOR
FSET
XTAL
OSC
XTAL1
XTAL2

FIG. 4

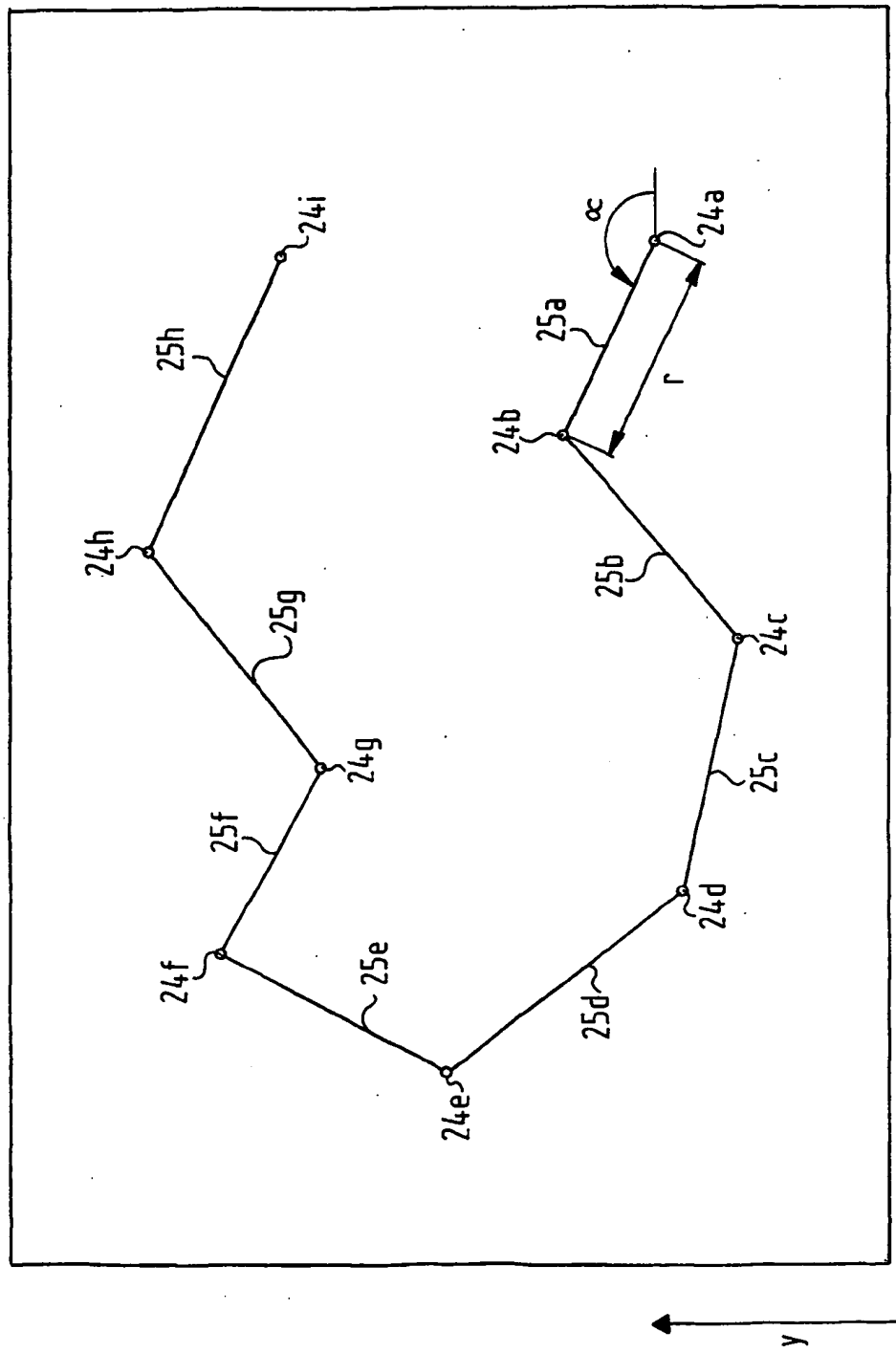

24i
25h
24h
25g
24g
25f
24f
25e
24e
25d
24d
25c
24c
25b
24b
25a
24a
α
r
x
y

FIG. 5

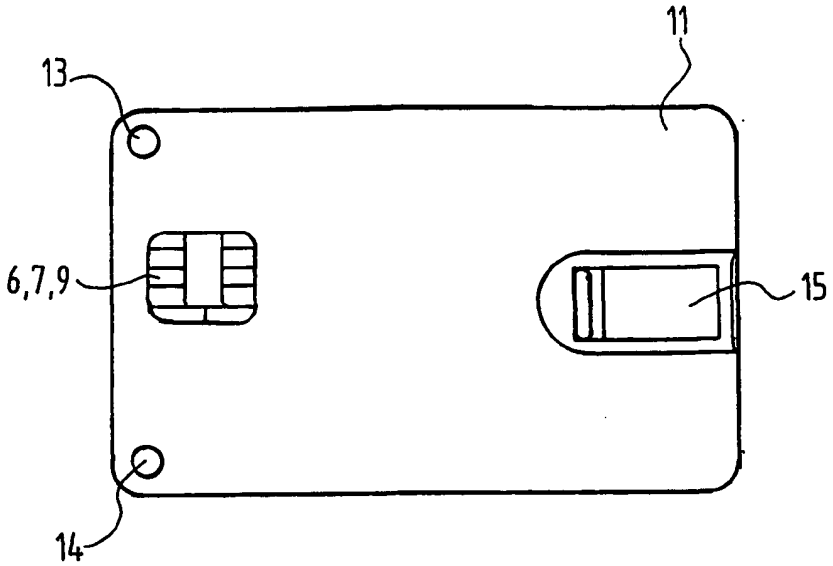


FIG. 6

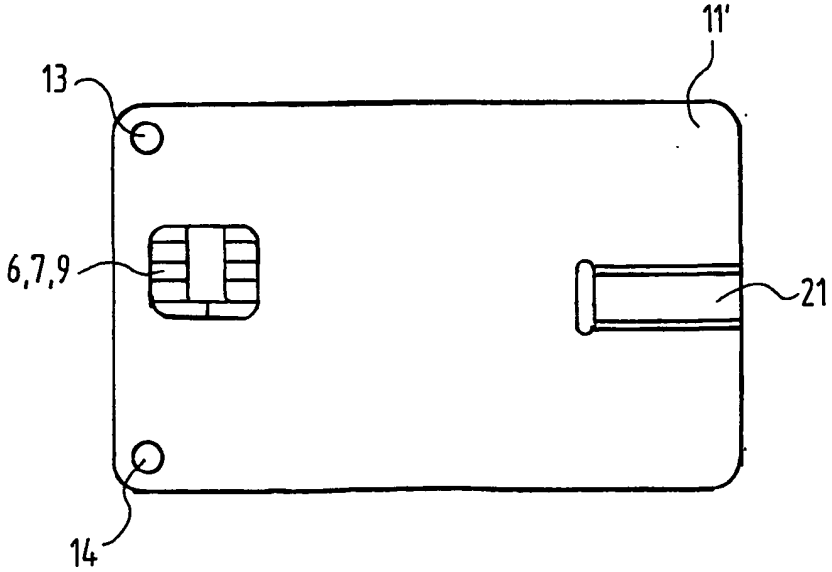


FIG. 7

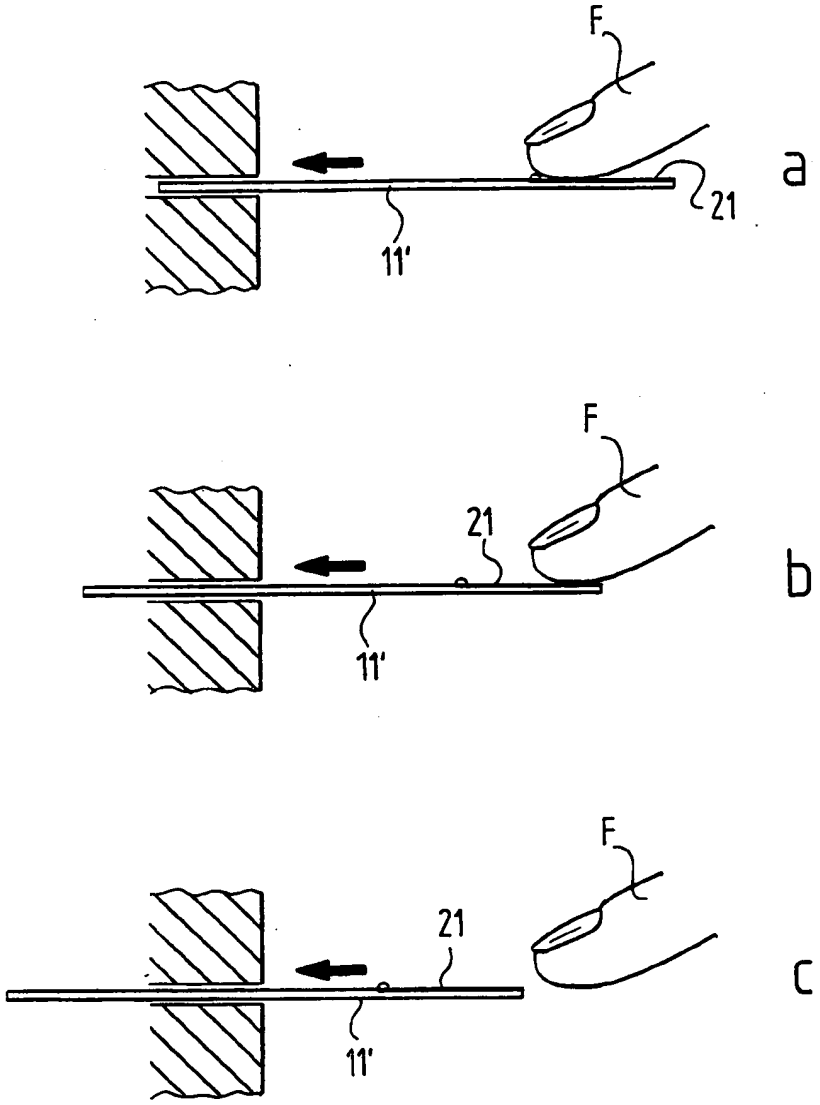


FIG. 8

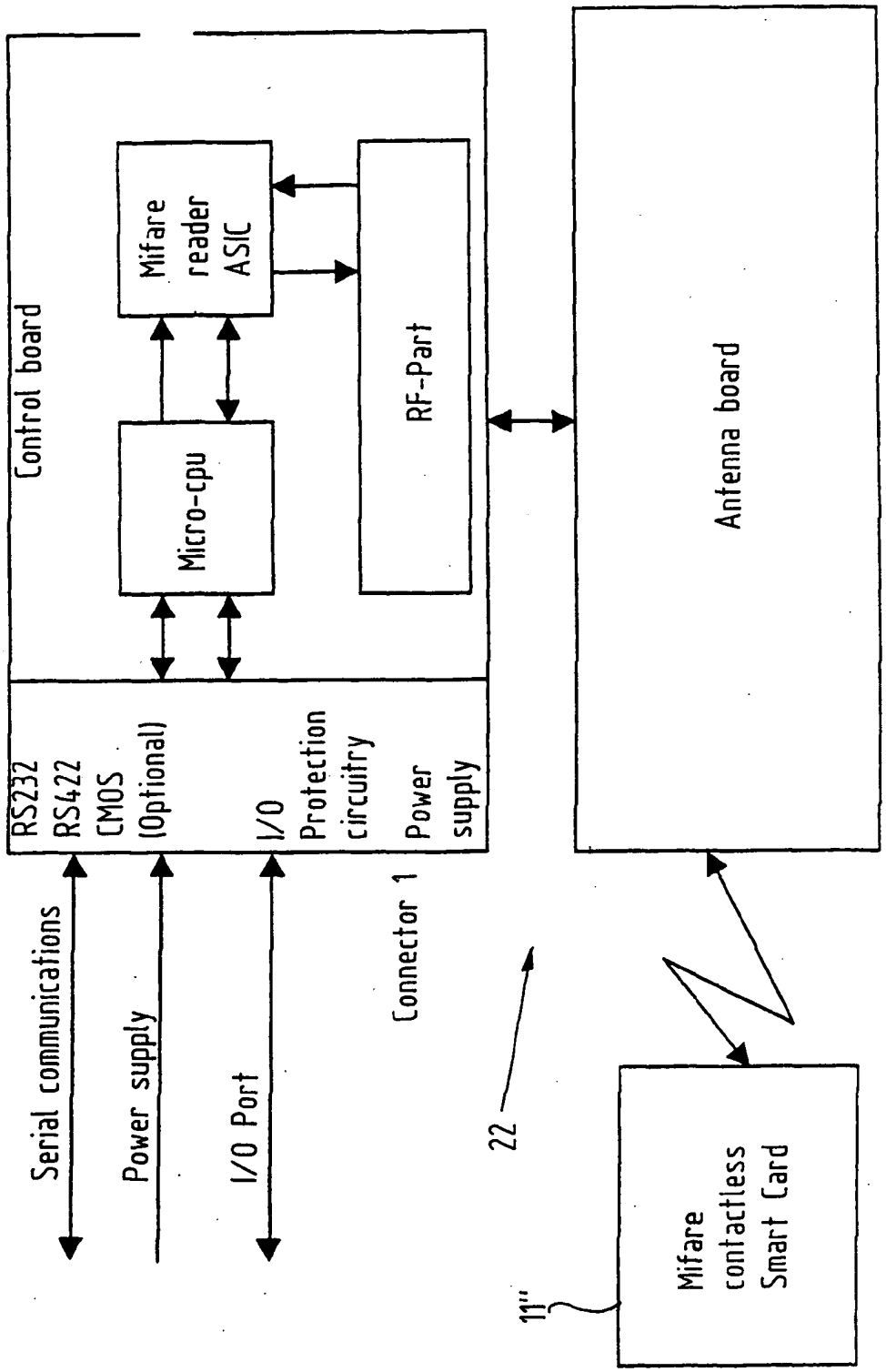

Control board
Mifare reader ASIC
Micro-cpu
RF-Part
Antenna board
RS232
RS422
CMOS
(Optional)
I/O Protection circuitry
Power supply
Connector 1
Serial communications
Power supply
I/O Port
22
11''
Mifare contactless Smart Card

FIG. 9

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/04235

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 994 439 A (SONY CORP) 19 April 2000 (2000-04-19) abstract; claims; figures column 3, line 8 -column 4, line 22 column 10, line 20 -column 13, line 13	1-7, 9-20,22, 24-30
Y	---	8,21
X	DE 196 18 144 C (ZIEGLER HANS BERNDT DR) 10 April 1997 (1997-04-10) the whole document	1-4,7, 11-17, 20,22, 24-26,30

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 September 2002	09/09/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Meyl, D

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/04235

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 623 552 A (LANE WILLIAM F) 22 April 1997 (1997-04-22) abstract; claims; figures column 4, line 59 -column 10, line 3	1-4,7, 9-18,20, 22-24
X	GB 2 181 582 A (BLACKWELL VICTOR CAMPBELL) 23 April 1987 (1987-04-23) page 1, line 66 -page 2, line 28 page 2, line 89 -page 3, line 73; figures	1-4,7, 9-16,20, 22-30
X	PATENT ABSTRACTS OF JAPAN vol. 016, no. 085 (P-1319), 28 February 1992 (1992-02-28) & JP 03 269694 A (MITSUBISHI ELECTRIC CORP), 2 December 1991 (1991-12-02) abstract	1-4,7,9, 11-17, 20,24-30
Y	WO 99 43258 A (IDEX AS ;TSCHUDI JON (NO); MATHIASSEN IVAR (NO); JOHANSEN IB RUNE) 2 September 1999 (1999-09-02) abstract; claims; figures	8,21
A	DE 196 48 767 A (SIEMENS AG OESTERREICH) 26 June 1997 (1997-06-26) the whole document	1-30
A	EP 0 833 281 A (SAGEM) 1 April 1998 (1998-04-01) abstract; claims; figure	1,13
A	WO 98 01820 A (DYNAMIC DATA SYSTEMS PTY LTD ;ELBAUM HECTOR DANIEL (AU)) 15 January 1998 (1998-01-15) abstract; claims; figures page 2, line 12 -page 7, line 4	1,2,7, 12-14, 17,20, 25,26
A	EP 1 045 346 A (OMRON TATEISI ELECTRONICS CO) 18 October 2000 (2000-10-18) column 4, line 12 -column 8, line 40; figures	1,5,13, 18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 02/04235

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0994439	A	19-04-2000	JP 2000123144 A		28-04-2000
			EP 0994439 A2		19-04-2000
DE 19618144	C	10-04-1997	DE 19618144 C1		10-04-1997
US 5623552	A	22-04-1997	NONE		
GB 2181582	A	23-04-1987	AU 6476786 A		05-05-1987
			EP 0241504 A1		21-10-1987
			WO 8702491 A1		23-04-1987
JP 03269694	A	02-12-1991	JP 2118521 C		06-12-1996
			JP 8031146 B		27-03-1996
WO 9943258	A	02-09-1999	NO 980827 A		27-08-1999
			AU 2442899 A		15-09-1999
			EP 1058513 A1		13-12-2000
			JP 2002504388 T		12-02-2002
			WO 9943258 A1		02-09-1999
DE 19648767	A	26-06-1997	AT 405218 B		25-06-1999
			AT 208495 A		15-10-1998
			DE 19648767 A1		26-06-1997
EP 0833281	A	01-04-1998	FR 2752976 A1		06-03-1998
			EP 0833281 A1		01-04-1998
WO 9801820	A	15-01-1998	AU 3248997 A		02-02-1998
			WO 9801820 A1		15-01-1998
EP 1045346	A	18-10-2000	JP 2000268175 A		29-09-2000
			EP 1045346 A2		18-10-2000